

Auftragsverarbeiter und Verantwortlicher – ein Abgrenzungsversuch

A. Arbeitsteiliges Verhalten und Rollen im Datenschutzrecht:

Arbeitsteiliges Verarbeiten von personenbezogenen Daten ist Realität, sei es zB ausgelagerte Speicherung oder Aktenvernichtung oder auch die Erhebung von Daten zB für Marketingzwecke durch Dritte. Eine datenverarbeitende Organisation ist entweder „Verantwortlicher“ oder „Auftragsverarbeiter“, aber nicht beides gleichzeitig.

„**Verantwortlicher**“ (Definition lt. Art 4 Z 7 DSGVO) ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

„**Auftragsverarbeiter**“ (Definition lt. Art 4 Z 8 DSGVO) eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Bestimmte Regelungen der DSGVO treffen nur Verantwortliche, und schreiben diesem bestimmte Verhaltensweisen vor; hier einige Beispiele von Verpflichtungen, die nur Verantwortliche, nicht aber Auftragsverarbeiter treffen:

- **Rechtmäßigkeit** der Verarbeitung der Daten iSd Art 6, Art 9 oder Art 10 DSGVO,
- **Informationspflicht** iSd Art 13 oder Art 14 DSGVO gegenüber den Betroffenen
- **Wahrnehmung der Rechte der betroffenen Personen**

B. Ist jede Datenweitergabe mit einem Auftragsverarbeitungsvertrag abzusichern?

Werden Daten auf vertraglicher Basis von einem Verantwortlichen **an einen Empfänger weitergegeben** (übermittelt), dann stellt sich oft die Frage, ob der Empfänger der Daten, der mit den Daten auch gewisse Verarbeitungen zur Erfüllung seiner Leistungsverpflichtung durchführt, ein Auftragsverarbeiter ist, oder nicht.

Der Auftragsverarbeiter nimmt dem Verantwortlichen einen Teil dessen eigener Verarbeitungstätigkeit ab, und führt diese „im Auftrag“ für diesen durch; er hat keinen eigenen Zweck für diese Verarbeitung, und auch der Inhalt der Daten ist für seine Tätigkeit nur von untergeordneter Relevanz.

Eine weitere Möglichkeit nach den Bestimmungen der DSGVO in der arbeitsteiligen Datenverarbeitung sind sog. „**gemeinsame Verantwortliche**“ iSd Art 26 DSGVO, bei der zwei oder mehr (eigenständige) Verantwortliche gemeinsam mit vertraglich definierten Verantwortlichkeiten personenbezogene Daten verarbeiten. Ein Beispiel dafür wäre zB eine gemeinsam geführte Kunden- oder Marketingdatenbank oder eine gemeinsame Buchungsplattform von unterschiedlichen Reiseveranstalter und Unternehmen die Nebenleistungen anbieten (Hotels, Mietwagen, Veranstaltungsbuchung etc...).

Verfasser:

Dr. Thomas Schweiger, LL.M. (Duke)

CIPP/E, zertifizierter Datenschutzbeauftragter

Linz, 10.09.2018 21:47

Die entscheidende Frage ist, ob der Auftragsverarbeiter für einen Verantwortlichen eine Verarbeitungstätigkeit iSd DSGVO durchführt. Diese sind in der DSGVO umfassend definiert. Sie umfassen automatisierte oder nicht-automatisierte Vorgänge oder Vorgangsreihen im Zusammenhang mit personenbezogenen Daten wie das **Erheben**, das **Erfassen**, die **Organisation**, das **Ordnen**, die **Speicherung**, die **Anpassung** oder **Veränderung**, das **Auslesen**, das **Abfragen**, die **Verwendung**, die **Offenlegung** durch Übermittlung, **Verbreitung** oder eine andere Form der **Bereitstellung**, der **Abgleich** oder die **Verknüpfung**, die **Einschränkung**, das **Löschen** oder die **Vernichtung von personenbezogenen Daten von natürlichen Personen**.

Es muss sich bei der Tätigkeit u.a. um eine **zielgerichtete Verarbeitung** von personenbezogenen Daten **im Kernbereich** der Aufgabe des Verarbeiters für einen Verantwortlichen handeln, damit diese als Auftragsverarbeitung qualifiziert wird. Zusätzliche Aufgaben, die der Auftragsverarbeiter übernimmt, verändern die Beurteilung nicht. Verarbeitet die Organisation die Daten nur anlässlich eines Auftrages, der außerhalb des Kernbereiches einer Datenverarbeitung liegt, stellt dies vermutlich eine bloße Übermittlung der Daten an einen eigenen Verantwortlichen dar, der diese Daten benötigt, um eine inhaltlich definierte Aufgabe zu erbringen, die im Kernbereich keine Verarbeitungstätigkeit für den übermittelnden Verantwortlichen darstellt. Der Übermittlungsempfänger nutzt diese übermittelten Daten für einen eigenen Zweck, und eben nicht im Auftrag des übermittelnden Verantwortlichen.

Entscheidet der Verarbeiter selbst über den Einsatz von Mittel und Zweck der Verarbeitung der Daten iSd Art 4 Z 7 DSGVO. In der Abgrenzung ist es von wesentlicher Bedeutung, dass der Übermittlungsempfänger über die **Verarbeitungszwecke** entscheidet. Die Auswahl der technisch-organisatorischen Fragen der Verarbeitung kann auch delegiert werden.

Eine konkrete Stellungnahme der **Österreichischen Datenschutzbehörde** zur Abgrenzung ist im [Leitfaden](#) nicht erfolgt. Es kann auf die Veröffentlichungen in Deutschland zurückgegriffen werden; es ist jedoch zu berücksichtigen, dass die Rechtsfigur der sog. Funktionsübertragung in der DSGVO nicht umgesetzt wurde. Die DSK hat ein [Kurzpapier zur Auftragsverarbeitung](#) veröffentlicht, und auch die Bitkom veröffentlichte [Hinweise](#) dazu.

Nur eine **Kerntätigkeit des Auftragsverhältnisses in einer Verarbeitungstätigkeit iSd DSGVO führt zur Qualifikation als Auftragsverarbeiter für einen Verantwortlichen**. Zu denken ist zB an die Erhebung der Daten durch Dritte am einen Ende der Verarbeitungskette und an die datenschutzkonforme Entsorgung (Vernichtung) am anderen Ende derselben. Sämtliche dazwischenliegenden Verarbeitungsvorgänge, wie das Organisieren, die Aufbereitung, die Anreicherung von Daten. Es kann zB auch die Speicherung und Ablage der Daten oder ein Security-Backup oder das Löschen von Daten an einen Dritten als Auftragsverarbeiter ausgelagert werden.

C. Beispiele für Auftragsverarbeitungen

Die [Datenschutzkonferenz](#) und die [Bitkom](#) haben in ihren Papieren auch Beispiele angeführt; dies ist eine Zusammenfassung bzw. Anpassung an die österreichischen Verhältnisse.

Beispiele für Auftragsverarbeitungen:

- ...DV-technische Arbeiten für die Lohn- und Gehaltsabrechnung oder die Finanzbuchhaltung durch Rechenzentren
- ...externe Datenhaltung oder –speicherung, insbes. beim teilweisen oder gesamten Outsourcing eines Rechenzentrums sowie Storage- und Back-up-Lösungen
- ...Implementierung neuer IT-Systeme mit Migration von Echtdaten
- ...Outsourcing personenbezogener Datenverarbeitung im Rahmen von Cloud-Computing, ohne dass ein inhaltlicher Datenzugriff des Cloud-Betreibers erforderlich ist
- ...Werbeadressenverarbeitung in einem Letter Shop und externe Druckdienstleistungen unter Verwendung von personenbezogenen Daten
- ...Verarbeitung von Kundendaten durch ein Callcenter ohne wesentliche eigene Entscheidungsspielräume dort (Telefonmarketing, Kundenzufriedenheitsbefragungen)
- ...Auslagerung der E-Mail- Verwaltung oder von sonstigen Datendiensten zu Webseiten (z.B. Betreuung von Kontaktformularen oder Nutzeranfragen)
- ...Datenerfassung, Datenkonvertierung oder Einscannen von Dokumenten
- ...Auslagerung der Backup-Sicherheitspeicherung und anderer Archivierungen,
- ...Kundenakquise mit vorgegebenen Datenarten (zB zur Akquise von Spendern durch Beauftragte für NGOs)
- ...manueller oder elektronischer Archivierungsservice
- ...Datenträger- oder Papieraktenentsorgung durch Dienstleister
- ...Zentralisierung bestimmter „Share Services-Dienstleistungen“ innerhalb eines Konzerns, wie Dienstreisen-Planungen oder Reisekostenabrechnungen (jedenfalls sofern kein Fall gemeinsamer Verantwortlichkeit nach Art. 26 DS-GVO vorliegt)
- ...Apothekenrechenzentren
- ...ärztliche/zahnärztliche Verrechnungsstellen ohne Forderungsverkauf
- ...Sicherheitsdienste, die an der Pforte Besucher- und Anliefererdaten erheben
- ...externe Personen, Dienstleister, usw., die im Auftrag Betriebskosten in Miet- oder Eigentumswohnungen (Heizung, Strom, Wasser etc.) ablesen und/oder erfassen bzw. verarbeiten
- ...Visabeschaffungsdienstleister, die hierfür vom Arbeitgeber oder Reisebüro die Beschäftigtendaten erhalten

Beispiele, die nicht unter den Begriff Auftragsverarbeiter fallen:

- ...Tätigkeiten der Berufsgeheimnisträger (Steuerberater, Rechtsanwälte, externe Betriebsärzte, Wirtschaftsprüfer)
- ...Inkassobüros mit Forderungsübertragung
- ...Bankinstitute für den Geldtransfer
- ...Postdienste für den Brief- oder Pakettransport
- ...Tätigkeit als Hausverwaltung
- ...Detektive bei ihrer Observierungs-/ Überwachungs-/ Ausforschungstätigkeit
- ...Hersteller und Großhändler, die von Einzelhändlern für mit Endkunden vereinbarte Direktlieferungen die Endkundenadressen erhalten (beauftragte Warensendung)
- ...Blumen- oder Weinversender, die eine Liste mit Adressdaten zur Versendung der Blumen- bzw. Weingeschenke an dritte Personen erhalten (beauftragte Warensendung)
- ...Insolvenzverwalter
- ...Personalvermittlung nach Auftrag von Stellensuchenden oder Arbeitgebern (siehe dazu auch Beispiel 6 im WP 169)
- ...Internet-Plattformbetreiber zur Vermittlung zwischen Anbietern und Nachfragern, die sich auf der Plattform treffen können
- ...TKG-Dienstleistungen, es sei denn, darüberhinausgehende Zusatzdienste wie Auslagerung einer betrieblichen Telefonanlage oder Cloudspeicherlösungen usw.
- ...Versicherungs- /Finanzmakler, -vermittler im Rahmen des Kundenvertrags
- ...Handelsvertreter im Rahmen ihrer Beratungstätigkeit und Vertragsvermittlungen,
- ...Übersendung von Schulungsteilnehmer-Daten zur Durchführung der Schulung an einen externen Trainer, Schulungsveranstalter oder an das Tagungshotel
- ...Fertigung individueller medizinischer Produkte, Hilfsmittel, Prothesen etc. für Patienten/Kunden im Auftrag von Ärzten, Zahnärzten, Apotheken, Sanitätshäusern, Optikern usw.
- ...Medizinische Labore, Materiallabore usw. (Befundungen und Materialuntersuchung im Auftrag)
- ...Zahlungsdienstleister für elektronische Zahlungen (Transport von Zahlungsdaten, Geldwäsche- und Betrugsprüfung und den Mindestanforderungen der Finanzmarktregelungen)
- ...von Reisebüros aufgrund Kundenvertrags vermittelte Leistungsanbieter, wie Hotels, Mietwagenfirmen, Fluggesellschaften, Busunternehmen, Versicherungen usw.

D. Wie kann eine Abgrenzung erfolgen?

Unter Berücksichtigung der Hinweise der Bitkom könnten folgende Fragen, die sich ein Verantwortlicher stellt, zur Abgrenzung herangezogen werden:

1. Steht die **Verarbeitung von personenbezogenen Daten**, die der Verarbeiter von einem Auftraggeber erhält oder für den Auftraggeber erhebt, **im Mittelpunkt der Tätigkeit** (dh handelt es sich im Kernbereich um eine verarbeitungsrelevante Tätigkeit), oder steht ein anderer Leistungsinhalt im Vordergrund? Wenn der Leistungsinhalt „datengetrieben“ ist, dann kann eine Auftragsverarbeitung vorliegen, wenn ein anderer Leistungsinhalt im Vordergrund, dann ist eher davon auszugehen, dass eine Übermittlung an einen anderen Verantwortlichen vorliegt.
2. Hat der Verarbeiter „**Entscheidungsbefugnis**“ über die zu verarbeitenden Datenkategorien oder erhält er diesbezüglich eine Vorgabe von seinem Auftraggeber? Je mehr Entscheidungsbefugnis der Auftragnehmer hat, desto ist er Verantwortlicher iSd DSGVO.
3. Ist der Verarbeiter in Bezug auf Ausführung seiner Tätigkeit an **fachliche Weisungen** des Auftraggebers gebunden (**Eigenverantwortlichkeit**)? Wenn aufgrund der eigenen Stellung eine Weisungsbefugnis des Auftraggebers ausgeschlossen ist, dann wird die Tätigkeit eigenverantwortlich ausgeführt, und der Auftragnehmer ist Verantwortlicher iSd DSGVO.
4. Werden **nur Daten verarbeitet**, die vom Auftraggeber (oder von Dritter Seite auf Anweisung des Auftraggebers) **zur Verfügung gestellt werden** (außer bei der Erhebung von Daten)? Kommt es zB zu einer Anreicherung von Daten, die zur Verfügung gestellt werden, um neue Datenkategorien, bei denen die Daten dem Auftragnehmer bereits aufgrund seiner eigenen Tätigkeit zur Verfügung stehen (zB im zielgruppenorientierten Marketing), dann handelt es sich meist um mehrere gemeinsame Verantwortliche, die ihre Daten für einen bestimmten Zweck zusammen verwenden.
5. Ist es dem **Verarbeiter** gestattet, die **Daten für eigene Zwecke zu verarbeiten** und zu nutzen? Wenn der Verarbeiter bei Beendigung des Vertragsverhältnisses die Daten ohne Beeinträchtigung seiner eigenen Tätigkeit an den Auftraggeber herausgeben oder löschen kann, dann liegt meist Auftragsverarbeitung vor.
6. Besteht eine **vertragliche Beziehung** zu den betroffenen Personen? Der Auftragsverarbeiter steht in keinem Rechtsverhältnis zu den betroffenen Personen; sobald ein Vertragsverhältnis (Art 6 Abs 1 lit b DSGVO), eine Einwilligung (Art 6 Abs 1 lit a; Art 9 Abs 2 lit a DSGVO) oder eine andere taugliche Rechtsgrundlage für die Verarbeitung der Daten gegeben ist, besteht eine Stellung als Verantwortlicher.
7. Wie **tritt der Verarbeiter gegenüber den betroffenen Personen auf**? Der Außenkontakt des Verarbeiters in eigenem Namen gegenüber betroffenen Personen ist ein wesentliches Indiz für eine Stellung als Verantwortlicher. Wenn er jedoch im Namen des Vertragspartners an die Betroffenen Personen herantritt, oder und zB die Vertretung offenlegt, dann deutet das auf ein Auftragsverarbeitungsverhältnis hin.
8. Hat der Auftraggeber die Möglichkeit, die **Tätigkeit des Verarbeiters zu überwachen**? Wenn Audit-Rechte in Bezug auf die Art und Weise der Tätigkeit notwendigerweise vereinbart werden, dann weist dies auf eine Stellung als Auftragsverarbeiter hin.

E. Fernwartungszugriff und Prüfung oder Wartung von IT-Systemen als Auftragsverarbeitung

Oft wird dargelegt, dass ein Fernwartungszugriff, bei dem auch die Zugriffsmöglichkeit auf personenbezogene Daten besteht oder die Wartung von IT-Anlagen und IT-Systemen, bei der eine derartige Zugriffsmöglichkeit besteht, eine Auftragsverarbeitung iSd DSGVO darstellen. Dies wäre zB bei einem Unternehmen der Fall, welches Drucker oder Kopierer wartet oder repariert.

Bei Internetrecherchen kann festgestellt werden, dass diese Meinung vorwiegend in Deutschland vertreten wird. Sie basiert mE auf § 11 Abs 5 BDSG (alt), denn darin war festgelegt, dass die Regelungen für die Auftragsverarbeitung auf die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch Beauftragte anwendbar waren, wenn dabei ein Zugriff auf personenbezogene Daten nicht auszuschließen war.

Diese Regelung bedeutete jedoch nicht, dass es sich bei den Situationen, die in § 11 Abs 5 BDSG (alt) tatsächlich auch um Auftragsverarbeitung handelt; es wurden nur die Regelungen, die für die Auftragsverarbeitung bestanden haben, auf andere Sachverhalte angewendet, die aus Risikosicht eine ähnliche Problematik aufwiesen. Dadurch wurden diese Situationen nicht zur Auftragsverarbeitung.

In der DSGVO findet sich keine Regelung, die dem § 11 Abs 5 BDSG (alt) entsprechen. Wenn anlässlich der Fernwartung der IT-Systeme oder der Verarbeitungsanlagen potentiell Zugriff oder Lesezugriff auf die Daten von Betroffenen auf den Systemen des Auftraggebers genommen werden kann, dann ist dies mE nicht der Kernbereich einer bewussten Verarbeitungstätigkeit, sondern die Hauptleistung besteht in der Wartung.